

IntelCrawler

Intelligence Report

Lizard Squad / Guardian of Peace (GOP)

FOR PUBLIC RELEASE



Intelligence Request

Description	
INT-REQ-ID	INT-REQ-451
Background	<p>“Lizard Squad” is a group of hackers, responsible for DDoS attacks against:</p> <ul style="list-style-type: none"> - EA Games; - Xbox Live; - Sony Playstation Network; - RockStar Games. <p>“GOP” is a group of hackers, responsible for cyber attack against Sony.</p> <p>Analysis shows some linkage and correlation between “Lizard Squad” and so-called “GOP”. The details in the report may help attribution and some IOA’s may help defend future attacks.</p>
Priority	High
Target Date	Report Immediately When Available

Table of Contents

Intelligence Request	2
Table of Contents.....	3
Adversary Profiles	4
Lizard Squad	4
“abdilo”	4
“lolaristocrat”.....	9
Chronological Analysis	12
August 24 th 2014	12
August 26 th 2014	12
November 21 th 2014	13
November 24 th 2014	13
November 26 th 2014	15
December 1 st 2014 - “I am the boss of G.O.P.”	15
December 3 st 2014 - “We have released the data of Sony Pictures here”	16
December 5 st 2014 - “I am the head of GOP”.....	16
December 6 th 2014 - “Gift of GOP for 2nd day”	16
December 7 th 2014 - “Gift of GOP for 3rd day Financial data of Sony Pictures” ..	17
December 8 th 2014 - “Gift of GOP for 4th day”	17
December 10 th 2014 - “Gift of Sony for 5th day: My Life At The Company-Part 1”	18
December 11 th 2014 - “Gift of Sony for 5th day: My Life At The Company-Part 2”	18
December 14 th 2014 - “The sooner SPE accept our demands, the better”	18
December 18 th 2014 - “Dear Sony from GOP”	19
December 19 th 2014 - “Message to CEO of Sony - Michael Lynton”	20
December 20 th 2014 - “Christmas gift to FBI”	22
December 22 th 2014 - “Working together with GOP on a Christmas project” ..	22
December 29 th 2014 - “Well, we do know some people from the GOP”	25
December 30 th 2014 - “Looking at this south korean powerplant”	25
December 31 th 2014 - “Suicide Hacking in Australia”	26
A.1.....	28
January 3 ^d 2015 - “GOP: Final message to Sony and world”	31
Appendix A. - Lizard Squad / GOP Characteristics	32
Appendix B. - Social Graph.....	34
Conclusion.....	35
Disclaimer	36

Adversary Profiles

Lizard Squad

Lizard Squad is a group of cybercriminals, having 8 key members – “dragon”, “komodo”, “ryan” (was arrested), “sp3c”, “adbilo”, “chameleon”, “vagineer” or “vinnie” (was arrested), & “gecko”. This group started to position themselves as Hacktivists, attacking big corporations, primarily gaming servers. There are also several other bad actors which appeared after the first cyber attacks of the group, such as “ice”, “MLT”, “alg0d”, “jordie” (was arrested), “teridax” and “lolaristocrat”, who allegedly acted as one of the main operators on their IRC channel.

The group has several technical leaders, as well as some ideological support, having no ties to cyber attacks or practical hacking. One of the first cyber attacks on behalf of the group was performed against the Sony Playstation Network, and several other corporations. Since these first attacks, the profile of the group has significantly changed.

Some of their key members, such as “Abdilo” and “lolaristocrat” have become more independent, performing cyber attacks against military, government and private sector network resources without any clear motivation. There are several identified Twitter accounts with the hashtag #KimJongSec, created by the last bad actor for reasons unknown. The account promotes DDoS attacks against South Korea and their President’s WEB-site.

As of October 2014, “Abdilo” left Lizard Squad per his postings, but retained some relations with its key members. Later in December 2014, “Abdilo” also published several posts supporting North Korea, while continually showing aggression against the US and Australian Government.

He also attacked one of the biggest nuclear energy companies in South Korea - Korea Hydro & Nuclear Power (KHNP)¹², targeting their power plant infrastructure, where "non-critical" data seemed to have been stolen. Before the attacks against South Korea, “Abdilo” had compromised several government resources of the US and Australia Government.

“abdilo”

In one of the messages from Lizard Squad, a nickname of “Abdilo” appears:

¹ <http://www.reuters.com/article/2014/12/22/us-southkorea-nuclear-idUSKBN0K008E20141222>

² <http://www.reuters.com/article/2014/12/30/nuclear-southkorea-cybersecurity-idUSL3N0UE1A320141230>

"Little thieves are hanged, but great ones escape."

We set out on our journey 2 weeks ago with the plan to cause havoc within the gaming community. Our motives varied throughout this adventure. Originally it was to see if we could evade being caught and to experience the raw thrill of anarchy, not being bound to phony laws. We've been called everything from an organized criminal "gang" to complete assholes, really we are just a bunch of guys with too much free time. Throughout our journey we met new people, gained new members, learned new things. People tried taking swings at us (and missed). We proved that even though we are little in this very big world, that a small group of friends who work together can cause a lot of havoc without legal repercussions. Today we will be disbanding, behind the green reptiles and other bullshit, we have lives believe it or not, things to do, people to meet.

Goodbye.

- dragon
- Komodo
- ryan
- sp3c
- **abdilo**
- Chameleon
- Vagineer
- Gecko

PS: chF was never apart of LizardSquad, just a friend.

Pic.1 – The key members of Lizard Squad. This list will change later, as some members will leave the group, and new Hacktivists join the group

Using operatives and networked resources, discovery revealed that the domain name "lizardsquad.ru" was registered on the following e-mail - surivaton@gmail.com.

Later, "Abdilo" explains, that he was the owner of this domain name, but after some time, left the group.

I joined back in august, messed around and I hosted lizardsquad.ru and lizardsquad.com. I never had control of the ddos botnet. Left lizardsquad back in october but still talk with the members. One of lizardsquad's members used one of my domain accounts to register lizardpatrol.com (thus linking one of my old emails with lizardpatrol). (December 31st, "Abdilo")³

³ <http://pastebin.com/DvSf6dAK>

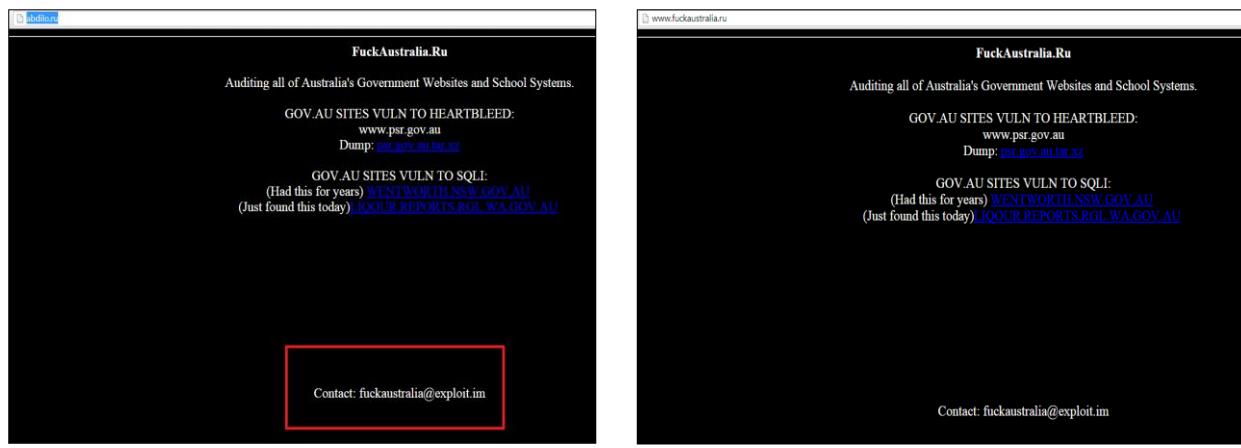
Pic.2 – One of the official domain names of Lizard Squad

“abdilo”	
Lastname	Crees
Firstname	David
E-Mail	surivaton@gmail.com
Accounts	Facebook https://www.facebook.com/ARMHF?ref=ts (“Root Toor”); GitHub https://github.com/surivaton (“David Crees”); YouTube https://www.youtube.com/watch?v=M7TnYo7pnkA ; Google Plus https://plus.google.com/116092303179922520941/posts ; Reddit https://www.reddit.com/user/surivaton
Location	Gladstone, Queensland, Australia Calliope, Australia
Skype	Skype: “facebook:surivaton”
Jabber	abdilo@exploit.im abdilo@darkcode.com
Nicknames	Abdilo, Notavirus, Surivaton, Grey Hat Mafias Bitch
Profiles	Hackforums: http://webcache.googleusercontent.com/search?q=cache:BYOA0DBtjPAJ:www.hackforums.net/showthread.php%3Ftid%3D4331159%26page%3D15+&cd=18&hl=en&ct=clnk&gl=ru P0wersurge.com: https://www.p0wersurge.com/forums/introductions/12879-hi/

	Exploit.in: https://exploit.in/forum/index.php?showuser=55603
Comments	Had agoraphobia during childhood WEB-applications hacking, Botnets Hacking AUTism is mentioned on one of his profiles

Table 1 – “Abdilo” Profile

Besides the identified Lizard Squad’s domain name, there were other identified domain names registered by this bad actor in the past, using the same e-mail and details:



The image contains two screenshots of web pages. The left screenshot is from 'Abdilo.ru' and the right is from 'Fuckaustralia.ru'. Both pages have a black background with white text. They both display the following content:

FuckAustralia.Ru
Auditing all of Australia's Government Websites and School Systems.
GOV.AU SITES VULN TO HEARTBLEED:
www.psr.gov.au
Dump: <http://www.psr.gov.au/xx>
GOV.AU SITES VULN TO SQLI:
(Had this for years) WENTWORTH.NSW.GOV.AU
(Just found this today) OUR.REPORTS.RGL.WA.GOV.AU

At the bottom of each page, there is a red box containing the contact information: 'Contact: fuckaustralia@exploit.im'.

Abdilo.ru **Fuckaustralia.ru**

Pic.3 – Domain names, owned by “Abdilo”, had Jabber contact: fuckaustralia@exploit.im and information about vulnerabilities on Australian government WEB-resources

In March 2014, the identified bad actor published information about SSL vulnerabilities⁴ in Juniper devices, exposing vulnerable network resources:

- extranet.uphs.upenn.edu;
- vpn.stloiscountymn.gov;
- vpn1.broadcastaustralia.com.au;
- remote.compumenn.com.au;
- rna.n.nsa.nexus.telstra.com.au.

The same resources, which include “stolen lists from @playstation.sony.com”, were traded on the black market by a bad actor, having the nickname “FAKBEN”⁵.

⁴ <http://www.div-13.com/view/7c5afed3>

⁵ <http://i25c62nvu4cgeqyz.onion/profile.php?id=9490>

Index - Other Vendors - Heartbleed dump of telstra.com(Big Australian ISP)

Pages: 1		Post reply
FAKBEN	2014-08-06 06:29:27	#1
Vendor	logins, information, private details, cookies, ssl/vpn, \$1200, (\$1200 because no one in the world has ever broken into Telstra.com) http://k5zq47j6wd3wdvjq.onion/listing/31153	
From: Honolulu Registered: 2014-07-23 Posts: 104 🕒 PM		
Offline		Quote
Pages: 1		Post reply

Index - Other Vendors - Heartbleed dump of telstra.com(Big Australian ISP)

Index - Other Vendors - New SSLVPN 15.5MB HEARTBLEED DUMP FOR EXTRANET.UPHS.UPENN.EDU

Pages: 1		Post reply
FAKBEN	2014-08-10 17:38:26	#1
Vendor	is the dump not just the login details like it is the dump that I got the login details from, that I dumped SSN, DOB, DEATH RECORDS, CORPORATE INFORMATION, COOKIES, PRIVATE DOCUMENTS, INTRANET, CITRIX, RDP, SSLVPN username and passwords emails	
From: Honolulu Registered: 2014-07-23 Posts: 104 🕒 PM		
Offline		-----> 900\$ <-----
Pages: 1		Post reply

Index - Other Vendors - New SSLVPN 15.5MB HEARTBLEED DUMP FOR EXTRANET.UPHS.UPENN.EDU

Index - Other Vendors - Private list stolen @playstation.sony.com

Pages: 1		Post reply
FAKBEN	2014-09-11 21:01:09	#1
Vendor	Description PUB_REL_ID, FIRST_NAME, LAST_NAME, EMAIL_ADDRESS, DEPARTMENT_GROUP, GROUP_HEAD from @playstation.sony.com. -----> Perfect for social engineering and ip grabbing. Private list stolen and all are valid	
From: Honolulu Registered: 2014-07-23 Posts: 104 🕒 PM		
Offline		Quote
kr151un	2014-09-16 15:19:09	#2
Member	I am interested, sent you PM but you didn't reply me.	
From: Honolulu Registered: 2014-05-07 Posts: 1 🕒 PM		
Offline		Quote

Pages: 1		Post reply
evolution	All	Search for...
sgt 100\$ gov 100 edu		
mo.gov virginia.gov louisiana.gov		
gatech.edu uky.edu vmi.edu miami.edu berkeley.edu case.edu utep.edu warburgseminary.edu thscsa.edu covenant.edu hws.edu nche.edu uoregon.edu csuchico.edu csusfresno.edu		
louisville.edu ncisu.edu		
rutgers.edu ncmc.edu spsli.edu sru.edu nonwalk.edu ufl.edu iecu.edu iupui.edu		
cnr.edu		

Database info 400351 Records		
USERNAME, VERSION_DATE, ADDED_ID, ACTIVE, PASSWORD, FIRST_NAME, LAST_NAME,		
EMAIL, SEX, PHONE, STREET, CITY, STATE, ZIP, BIRTH_DATE, SITE_ID, COMM_PREF_ID, DELETED, LOCKED, CREDENTIAL, EMPLOYEE_ID, PN, OLD_ACCOUNT_ID		

Private list stolen @playstation.sony.com		
PUB_REL_ID, FIRST_NAME, LAST_NAME, EMAIL_ADDRESS, DEPARTMENT_GROUP, GROUP_HEAD from @playstation.sony.com Perfect for social engineering and ip grabbing		
Private list stolen and all are valid.		

Service Coding		

Clickbot + installation		

Botnet sell in MB		

Pic.4 – Identified bad actor “FAKBEN”, trading the same information as former Lizard Squad member “Abdilo” in the underground

The structure of the data has “DEPARTMENT_GROUP” and “GROUP_HEAD”, which might be related to internal corporate information from Sony network or one of their compromised applications, which may have housed employee data.

Index - Other Vendors - 680 k email + pass stolen

Pages: 1		Post reply
FAKBEN	2014-09-15 07:39:17	
Vendor	hotmail.com verizon.net yahoo.com gmail.com msn.com aol.com etc.. etc.. 680.000 email + pass	
From: Honolulu Registered: 2014-07-23 Posts: 104 🕒 PM		
Offline		

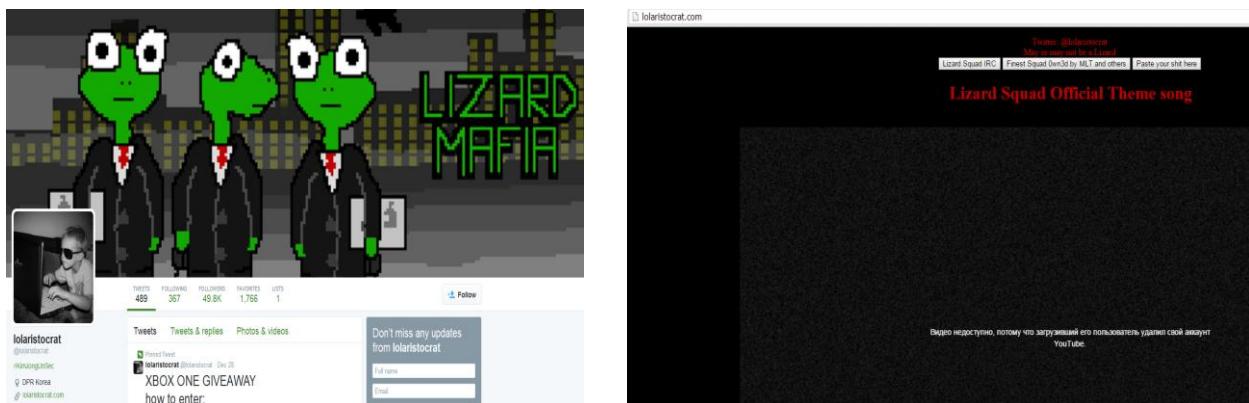
Pages: 1		Post reply
Email	Pass	
-----	-----	
1122 vdu51@verizon.net 1123 vdu51@verizon.net 1124 vdu51@verizon.net 1125 vdu51@verizon.net 1126 vdu51@verizon.net 1127 vdu51@verizon.net 1128 vdu51@verizon.net 1129 vdu51@verizon.net 1130 vdu51@verizon.net 1131 vdu51@verizon.net 1132 vdu51@verizon.net 1133 vdu51@verizon.net 1134 vdu51@verizon.net 1135 vdu51@verizon.net 1136 vdu51@verizon.net 1137 vdu51@verizon.net 1138 vdu51@verizon.net 1139 vdu51@verizon.net 1140 vdu51@verizon.net 1141 vdu51@verizon.net 1142 vdu51@verizon.net 1143 vdu51@verizon.net 1144 vdu51@verizon.net 1145 vdu51@verizon.net 1146 vdu51@verizon.net 1147 vdu51@verizon.net 1148 vdu51@verizon.net 1149 vdu51@verizon.net 1150 vdu51@verizon.net 1151 vdu51@verizon.net 1152 vdu51@verizon.net 1153 vdu51@verizon.net 1154 vdu51@verizon.net 1155 vdu51@verizon.net 1156 vdu51@verizon.net 1157 vdu51@verizon.net 1158 vdu51@verizon.net 1159 vdu51@verizon.net 1160 vdu51@verizon.net 1161 vdu51@verizon.net 1162 vdu51@verizon.net 1163 vdu51@verizon.net 1164 vdu51@verizon.net 1165 vdu51@verizon.net 1166 vdu51@verizon.net 1167 vdu51@verizon.net 1168 vdu51@verizon.net 1169 vdu51@verizon.net 1170 vdu51@verizon.net 1171 vdu51@verizon.net 1172 vdu51@verizon.net 1173 vdu51@verizon.net 1174 vdu51@verizon.net 1175 vdu51@verizon.net 1176 vdu51@verizon.net 1177 vdu51@verizon.net 1178 vdu51@verizon.net 1179 vdu51@verizon.net 1180 vdu51@verizon.net 1181 vdu51@verizon.net 1182 vdu51@verizon.net 1183 vdu51@verizon.net 1184 vdu51@verizon.net 1185 vdu51@verizon.net 1186 vdu51@verizon.net 1187 vdu51@verizon.net 1188 vdu51@verizon.net 1189 vdu51@verizon.net 1190 vdu51@verizon.net 1191 vdu51@verizon.net 1192 vdu51@verizon.net 1193 vdu51@verizon.net 1194 vdu51@verizon.net 1195 vdu51@verizon.net 1196 vdu51@verizon.net 1197 vdu51@verizon.net 1198 vdu51@verizon.net 1199 vdu51@verizon.net 1200 vdu51@verizon.net 1201 vdu51@verizon.net 1202 vdu51@verizon.net 1203 vdu51@verizon.net 1204 vdu51@verizon.net 1205 vdu51@verizon.net 1206 vdu51@verizon.net 1207 vdu51@verizon.net 1208 vdu51@verizon.net 1209 vdu51@verizon.net 1210 vdu51@verizon.net 1211 vdu51@verizon.net 1212 vdu51@verizon.net 1213 vdu51@verizon.net 1214 vdu51@verizon.net 1215 vdu51@verizon.net 1216 vdu51@verizon.net 1217 vdu51@verizon.net 1218 vdu51@verizon.net 1219 vdu51@verizon.net 1220 vdu51@verizon.net 1221 vdu51@verizon.net 1222 vdu51@verizon.net 1223 vdu51@verizon.net 1224 vdu51@verizon.net 1225 vdu51@verizon.net 1226 vdu51@verizon.net 1227 vdu51@verizon.net 1228 vdu51@verizon.net 1229 vdu51@verizon.net 1230 vdu51@verizon.net 1231 vdu51@verizon.net 1232 vdu51@verizon.net 1233 vdu51@verizon.net 1234 vdu51@verizon.net 1235 vdu51@verizon.net 1236 vdu51@verizon.net 1237 vdu51@verizon.net 1238 vdu51@verizon.net 1239 vdu51@verizon.net 1240 vdu51@verizon.net 1241 vdu51@verizon.net 1242 vdu51@verizon.net 1243 vdu51@verizon.net 1244 vdu51@verizon.net 1245 vdu51@verizon.net 1246 vdu51@verizon.net 1247 vdu51@verizon.net 1248 vdu51@verizon.net 1249 vdu51@verizon.net 1250 vdu51@verizon.net 1251 vdu51@verizon.net 1252 vdu51@verizon.net 1253 vdu51@verizon.net 1254 vdu51@verizon.net 1255 vdu51@verizon.net 1256 vdu51@verizon.net 1257 vdu51@verizon.net 1258 vdu51@verizon.net 1259 vdu51@verizon.net 1260 vdu51@verizon.net 1261 vdu51@verizon.net 1262 vdu51@verizon.net 1263 vdu51@verizon.net 1264 vdu51@verizon.net 1265 vdu51@verizon.net 1266 vdu51@verizon.net 1267 vdu51@verizon.net 1268 vdu51@verizon.net 1269 vdu51@verizon.net 1270 vdu51@verizon.net 1271 vdu51@verizon.net 1272 vdu51@verizon.net 1273 vdu51@verizon.net 1274 vdu51@verizon.net 1275 vdu51@verizon.net 1276 vdu51@verizon.net 1277 vdu51@verizon.net 1278 vdu51@verizon.net 1279 vdu51@verizon.net 1280 vdu51@verizon.net 1281 vdu51@verizon.net 1282 vdu51@verizon.net 1283 vdu51@verizon.net 1284 vdu51@verizon.net 1285 vdu51@verizon.net 1286 vdu51@verizon.net 1287 vdu51@verizon.net 1288 vdu51@verizon.net 1289 vdu51@verizon.net 1290 vdu51@verizon.net 1291 vdu51@verizon.net 1292 vdu51@verizon.net 1293 vdu51@verizon.net 1294 vdu51@verizon.net 1295 vdu51@verizon.net 1296 vdu51@verizon.net 1297 vdu51@verizon.net 1298 vdu51@verizon.net 1299 vdu51@verizon.net 1300 vdu51@verizon.net 1301 vdu51@verizon.net 1302 vdu51@verizon.net 1303 vdu51@verizon.net 1304 vdu51@verizon.net 1305 vdu51@verizon.net 1306 vdu51@verizon.net 1307 vdu51@verizon.net 1308 vdu51@verizon.net 1309 vdu51@verizon.net 1310 vdu51@verizon.net 1311 vdu51@verizon.net 1312 vdu51@verizon.net 1313 vdu51@verizon.net 1314 vdu51@verizon.net 1315 vdu51@verizon.net 1316 vdu51@verizon.net 1317 vdu51@verizon.net 1318 vdu51@verizon.net 1319 vdu51@verizon.net 1320 vdu51@verizon.net 1321 vdu51@verizon.net 1322 vdu51@verizon.net 1323 vdu51@verizon.net 1324 vdu51@verizon.net 1325 vdu51@verizon.net 1326 vdu51@verizon.net 1327 vdu51@verizon.net 1328 vdu51@verizon.net 1329 vdu51@verizon.net 1330 vdu51@verizon.net 1331 vdu51@verizon.net 1332 vdu51@verizon.net 1333 vdu51@verizon.net 1334 vdu51@verizon.net 1335 vdu51@verizon.net 1336 vdu51@verizon.net 1337 vdu51@verizon.net 1338 vdu51@verizon.net 1339 vdu51@verizon.net 1340 vdu51@verizon.net 1341 vdu51@verizon.net 1342 vdu51@verizon.net 1343 vdu51@verizon.net 1344 vdu51@verizon.net 1345 vdu51@verizon.net 1346 vdu51@verizon.net 1347 vdu51@verizon.net 1348 vdu51@verizon.net 1349 vdu51@verizon.net 1350 vdu51@verizon.net 1351 vdu51@verizon.net 1352 vdu51@verizon.net 1353 vdu51@verizon.net 1354 vdu51@verizon.net 1355 vdu51@verizon.net 1356 vdu51@verizon.net 1357 vdu51@verizon.net 1358 vdu51@verizon.net 1359 vdu51@verizon.net 1360 vdu51@verizon.net 1361 vdu51@verizon.net 1362 vdu51@verizon.net 1363 vdu51@verizon.net 1364 vdu51@verizon.net 1365 vdu51@verizon.net 1366 vdu51@verizon.net 1367 vdu51@verizon.net 1368 vdu51@verizon.net 1369 vdu51@verizon.net 1370 vdu51@verizon.net 1371 vdu51@verizon.net 1372 vdu51@verizon.net 1373 vdu51@verizon.net 1374 vdu51@verizon.net 1375 vdu51@verizon.net 1376 vdu51@verizon.net 1377 vdu51@verizon.net 1378 vdu51@verizon.net 1379 vdu51@verizon.net 1380 vdu51@verizon.net 1381 vdu51@verizon.net 1382 vdu51@verizon.net 1383 vdu51@verizon.net 1384 vdu51@verizon.net 1385 vdu51@verizon.net 1386 vdu51@verizon.net 1387 vdu51@verizon.net 1388 vdu51@verizon.net 1389 vdu51@verizon.net 1390 vdu51@verizon.net 1391 vdu51@verizon.net 1392 vdu51@verizon.net 1393 vdu51@verizon.net 1394 vdu51@verizon.net 1395 vdu51@verizon.net 1396 vdu51@verizon.net 1397 vdu51@verizon.net 1398 vdu51@verizon.net 1399 vdu51@verizon.net 1400 vdu51@verizon.net 1401 vdu51@verizon.net 1402 vdu51@verizon.net 1403 vdu51@verizon.net 1404 vdu51@verizon.net 1405 vdu51@verizon.net 1406 vdu51@verizon.net 1407 vdu51@verizon.net 1408 vdu51@verizon.net 1409 vdu51@verizon.net 1410 vdu51@verizon.net 1411 vdu51@verizon.net 1412 vdu51@verizon.net 1413 vdu51@verizon.net 1414 vdu51@verizon.net 1415 vdu51@verizon.net 1416 vdu51@verizon.net 1417 vdu51@verizon.net 1418 vdu51@verizon.net 1419 vdu51@verizon.net 1420 vdu51@verizon.net 1421 vdu51@verizon.net 1422 vdu51@verizon.net 1423 vdu51@verizon.net 1424 vdu51@verizon.net 1425 vdu51@verizon.net 1426 vdu51@verizon.net 1427 vdu51@verizon.net 1428 vdu51@verizon.net 1429 vdu51@verizon.net 1430 vdu51@verizon.net 1431 vdu51@verizon.net 1432 vdu51@verizon.net 1433 vdu51@verizon.net 1434 vdu51@verizon.net 1435 vdu51@verizon.net 1436 vdu51@verizon.net 1437 vdu51@verizon.net 1438 vdu51@verizon.net 1439 vdu51@verizon.net 1440 vdu51@verizon.net 1441 vdu51@verizon.net 1442 vdu51@verizon.net 1443 vdu51@verizon.net 1444 vdu51@verizon.net 1445 vdu51@verizon.net 1446 vdu51@verizon.net 1447 vdu51@verizon.net 1448 vdu51@verizon.net 1449 vdu51@verizon.net 1450 vdu51@verizon.net 1451 vdu51@verizon.net 1452 vdu51@verizon.net 1453 vdu51@verizon.net 1454 vdu51@verizon.net 1455 vdu51@verizon.net 1456 vdu51@verizon.net 1457 vdu51@verizon.net 1458 vdu51@verizon.net 1459 vdu51@verizon.net 1460 vdu51@verizon.net 1461 vdu51@verizon.net 1462 vdu51@verizon.net 1463 vdu51@verizon.net 1464 vdu51@verizon.net 1465 vdu51@verizon.net 1466 vdu51@verizon.net 1467 vdu51@verizon.net 1468 vdu51@verizon.net 1469 vdu51@verizon.net 1470 vdu51@verizon.net 1471 vdu51@verizon.net 1472 vdu51@verizon.net 1473 vdu51@verizon.net 1474 vdu51@verizon.net 1475 vdu51@verizon.net 1476 vdu51@verizon.net 1477 vdu51@verizon.net 1478 vdu51@verizon.net 1479 vdu51@verizon.net 1480 vdu51@verizon.net 1481 vdu51@verizon.net 1482 vdu51@verizon.net 1483 vdu51@verizon.net 1484 vdu51@verizon.net 1485 vdu51@verizon.net 1486 vdu51@verizon.net 1487 vdu51@verizon.net 1488 vdu51@verizon.net 1489 vdu51@verizon.net 1490 vdu51@verizon.net 1491 vdu51@verizon.net 1492 vdu51@verizon.net 1493 vdu51@verizon.net 1494 vdu51@verizon.net 1495 vdu51@verizon.net 1496 vdu51@verizon.net 1497 vdu51@verizon.net 1498 vdu51@verizon.net 1499 vdu51@verizon.net 1500 vdu51@verizon.net 1501 vdu51@verizon.net 1502 vdu51@verizon.net 1503 vdu51@verizon.net 1504 vdu51@verizon.net 1505 vdu51@verizon.net 1506 vdu51@verizon.net 1507 vdu51@verizon.net 1508 vdu51@verizon.net 1509 vdu51@verizon.net 1510 vdu51@verizon.net 1511 vdu51@verizon.net 1512 vdu51@verizon.net 1513 vdu51@verizon.net 1514 vdu51@verizon.net 1515 vdu51@verizon.net 1516 vdu51@verizon.net 1517 vdu51@verizon.net 1518 vdu51@verizon.net 1519 vdu51@verizon.net 1520 vdu51@verizon.net 1521 vdu51@verizon.net 1522 vdu51@verizon.net 1523 vdu51@verizon.net 1524 vdu51@verizon.net 1525 vdu51@verizon.net 1526 vdu51@verizon.net 1527 vdu51@verizon.net 1528 vdu51@verizon.net 1529 vdu51@verizon.net 1530 vdu51@verizon.net 1531 vdu51@verizon.net 1532 vdu51@verizon.net 1533 vdu51@verizon.net 1534 vdu51@verizon.net 1535 vdu51@verizon.net 1536 vdu51@verizon.net 1537 vdu51@verizon.net 1538 vdu51@verizon.net 1539 vdu51@verizon.net 1540 vdu51@verizon.net 1541 vdu51@verizon.net 1542 vdu51@verizon.net 1543 vdu51@verizon.net 1544 vdu51@verizon.net 1545 vdu51@verizon.net 1546 vdu51@verizon.net 1547 vdu51@verizon.net 1548 vdu51@verizon.net 1549 vdu51@verizon.net 1550 vdu51@verizon.net 1551 vdu51@verizon.net 1552 vdu51@verizon.net 1553 vdu51@verizon.net 1554 vdu51@verizon.net 1555 vdu51@verizon.net 1556 vdu51@verizon.net 1557 vdu51@verizon.net 1558 vdu51@verizon.net 1559 vdu51@verizon.net 1560 vdu51@verizon.net 1561 vdu51@verizon.net 1562 vdu51@verizon.net 1563 vdu51@verizon.net 1564 vdu51@verizon.net 1565 vdu51@verizon.net 1566 vdu51@verizon.net 1567 vdu51@verizon.net 1568 vdu51@verizon.net 1569 vdu51@verizon.net 1570 vdu51@verizon.net 1571 vdu51@verizon.net 1572 vdu51@verizon.net 1573 vdu51@verizon.net 1574 vdu51@verizon.net 1575 vdu51@verizon.net 1576 vdu51@verizon.net 1577 vdu51@verizon.net 1578 vdu51@verizon.net 1579 vdu51@verizon.net 1580 vdu51@verizon.net 1581 vdu51@verizon.net 1582 vdu51@verizon.net 1583 vdu51@verizon.net 1584 vdu51@verizon.net 1585 vdu51@verizon.net 1586 vdu51@verizon.net 1587 vdu51@verizon.net 1588 vdu51@verizon.net 1589 vdu51@verizon.net 1590 vdu51@verizon.net 1591 vdu51@verizon.net 1592 vdu51@verizon.net 1593 vdu51@verizon.net 1594 vdu51@verizon.net 1595 vdu51@verizon.net 1596 vdu51@verizon.net 1597 vdu51@verizon.net 1598 vdu51@verizon.net 1599 vdu51@verizon.net 1600 vdu51@verizon.net 1601 vdu51@verizon.net 1602 vdu51@verizon.net 1603 vdu51@verizon.net 1604 vdu51@verizon.net 1605 vdu51@verizon.net 1606 vdu51@verizon.net 1607 vdu51@verizon.net 1608 vdu51@verizon.net 1609 vdu51@verizon.net 1610 vdu51@verizon.net 1611 vdu51@verizon.net 1612 vdu51@verizon.net 1613 vdu51@verizon.net 1614 vdu51@verizon.net 1615 vdu51@verizon.net 1616 vdu51@verizon.net 1617 vdu51@verizon.net 1618 vdu51@verizon.net 1619 vdu51@verizon.net 1620 vdu51@verizon.net 1621 vdu51@verizon.net 1622 vdu51@verizon.net 1623 vdu51@verizon.net 1624 vdu51@verizon.net 1625 vdu51@verizon.net 1626 vdu51@verizon.net 1627 vdu51@verizon.net 1628 vdu51@verizon.net 1629 vdu51@verizon.net 1630 vdu51@verizon.net 1631 vdu51@verizon.net 1632 vdu51@verizon.net 1633 vdu51@verizon.net 1634 vdu51@verizon.net 1635 vdu51@verizon.net 1636 vdu51@verizon.net 1637 vdu51@verizon.net 1638 vdu51@verizon.net 1639 vdu51@verizon.net 1640 vdu51@verizon.net 1641 vdu51@verizon.net 1642 vdu51@verizon.net 1643 vdu51@verizon.net 1644 vdu51@verizon.net 1645 vdu51@verizon.net 1646 vdu51@verizon.net 1647 vdu51@verizon.net 1648 vdu51@verizon.net 1649 vdu51@verizon.net 1650 vdu51@verizon.net 1651 vdu51@verizon.net 1652 vdu51@verizon.net 1653 vdu51@verizon.net 1654 vdu51@verizon.net 1655 vdu51@verizon.net 1656 vdu51@verizon.net 16		

In one of the articles related to the first DDoS attacks on big e-gaming services, there was a mention of the bad actor “GOPGangster”⁶, who released some details about the incident. Lizard Squad member “Abdilo”, commented on the article using one of his old nicknames.

“Hundreds of people started to post about compromised accounts. One thread, from a user named GOPGangster, detailed how it happened. On Aug. 20, Jason contacted him and threatened to take over his account. “I didn’t believe him until my account was taken,” GOPGangster wrote. He knew he “was screwed,” he said, when his friend asked him why he left his ranked team. His account then wrote “I am God, Jason,” and transferred to Riot’s Oceania server. The password to the account was long and included “lots of random things that would be very difficult to grab,” GOP Gangster recalled. “Worst of all my account had my credit card info saved.”

“lolaristocrat”

“Lolaristocrat” has referenced DPR (North Korea) in his Twitter account, clearly written in English. According to analysts, this bad actor created several Twitter accounts, some time ago.



<https://twitter.com/lolaristocrat> (Twitter)

<http://lolaristocrat.com/> (WEB-site)

Pic.6 – Twitter and personal WEB-site of “lolaristocrat”

Three Twitter accounts have been identified with hashtag “#KimJongSec”, followed by two Lizard Squad members – “Abdilo” and “alg0d”.

⁶ <http://www.dailydot.com/esports/jason-shane-duffy-league-of-legends-hacks/>

Results for #KimJongSec

Top / All

People - View all

lolaristocrat

You've reached the end of the Top Tweets for #KimJongSec.

View all Tweets.

[https://twitter.com/KimJongSec \(new\)](https://twitter.com/KimJongSec (new))

[https://twitter.com/PacketoPortal \(old\)](https://twitter.com/PacketoPortal (old))

Pic.7 – Identified Twitter accounts with hashtag “KimJongSec” and link to Lizard Squad member “lolaristocrat”

Previously, the “KimJongSec” account had the name “K.J.U⁷. INFERNO”, publishing DDoS attacks against South Korean WEB-sites, including the official site of the President.

Pic.8 – Old Twitter account, maintained by user “labeled”

⁷ K.J.U – “KimJongUnSec”

The initial account belonged to Twitter with the username “labeiied”⁸, which appears to be an alias to an account of the Hacktivists using nickname “labelled” (“anon wjb”, “iadykiller”).

I only ever DDoS when i'm high. @KimJongSec

Pic.9 – The identified account of “labelled” also contained posts about Sony

⁸ <http://webcache.googleusercontent.com/search?q=cache:CuzuGryNM-0J:https://www.toptweet.org/user/labeiied+&cd=6&hl=en&ct=clnk&gl=uk>

Chronological Analysis

August 24th 2014

Lizard Squad published the message, directly addressed to Sony⁹ (11:03 AM):



Today we planted the ISIS flag on @Sony's servers #ISIS #jihad

11:03 AM - 24 Aug 2014

RETWEETS 523 FAVORITES 197

Flag media

1:29 PM - 24 Aug 2014

RETWEETS 84 FAVORITES 49

Pic.10 – Lizard Squad has threatened a Sony executive with a fake post about explosives in the plane

The same day, 1:29 PM, Lizard Squad tweeted at American Airlines saying that a flight carrying John Smedley, president of Sony Online Entertainment had "explosives on-board".

August 26th 2014

Lizard Squad performed DDoS against Sony PSN and published several messages addressed to Sony. As a defense, one of the posts contained references to monetary gain. This post demonstrates concern regarding Sony's costs for defense:

“Sony, yet another large company, but they aren't spending the waves of cash they obtain on their customers' PSN service. End the greed.” — Lizard Squad (@LizardSquad) August 24, 2014

HEY @Sony PICK UP THE PHONE

— Lizard Squad (@LizardSquad) *August 26, 2014*

⁹ <http://abcnews.go.com/Technology/lizard-squad-group-claiming-responsibility-high-profile-hacks/story?id=25129458>

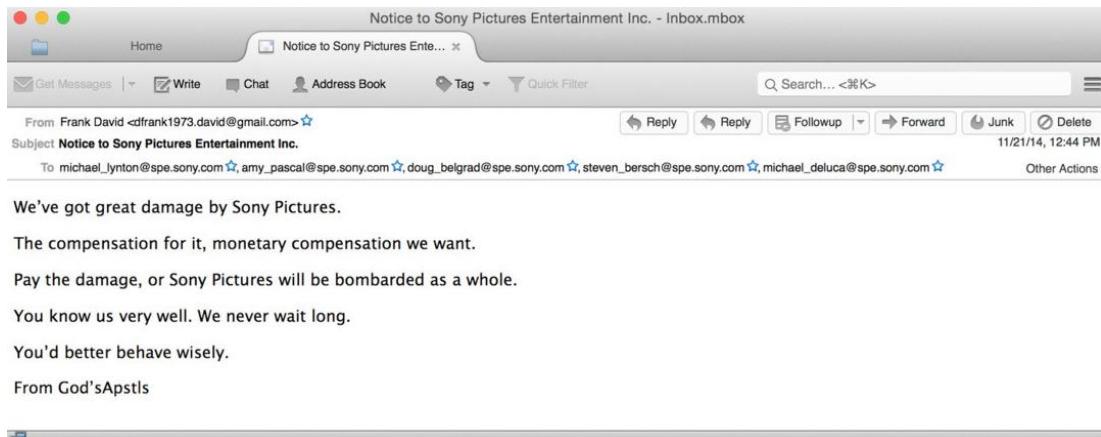
YO [@Sony](#) can we get estimates on how many \$ you paid for [@prolexic](#)?

— Lizard Squad (@LizardSquad) [August 26, 2014](#)

Pic.11 – The majority of Lizard Squad posts are directly addressed to Sony

November 21th 2014

During the initial stage, GOP sent a letter to Sony, asking for monetary compensation to prevent the leak:



Pic.12 – Anonymous hackers from GOP asked for monetary compensation from Sony

November 24th 2014

GOP provided Sony with a deadline, November 24th:



Pic.13 – GOP announced a deadline for Sony

These posts did not contain any information about the film “The Interview”.

Previously, the attackers posted to at least three Twitter feeds, leaving the same message: “*You, the criminals including [Sony Pictures CEO] Michael Lynton will surely go to hell. Nobody can help you.*” The image posted with the message shows a digitally edited image of Lynton’s head in a dark, hellish landscape.

 **soul Surfer** @SoulSurferMovie · 2h
Hacked By #GOP
 You, the criminals including Michael Lynton will surely go to hell.
 Nobody can help you.



Pic.14 – GOP published a negative post in hacked Twitter accounts about a Sony executive

The links on the leaked files were published in social networks and uploaded on Torrents.

November 26th 2014

The GOP leader published the following message:

posted *DS* 10:23 PM Wednesday, November 26, 2014 Greenwich Mean Time (GMT)

cut/paste *****

RE: To The Guardians Of Peace

From: godsapstls.boss4@unseen.is

Date: 2014-11-26 17:11

I am the head of GOP.

I appreciate you for calling us.

The data will soon get there.

You can find what we do on the following link.

<https://www.facebook.com/pages/The-Guardians-Of-Peace/604245239697994>

God bless us.

God's Apostles

Pic.15 – Anonymous hackers sent an e-mail to Sony

December 1st 2014 - “I am the boss of G.O.P.”

GOP published a message about stolen data:

I am the boss of G.O.P. A few days ago, we told you the fact that we had released some of Sony Pictures Bilm including Annie, Fury and Still Alice to the web. Those can be easily obtained through internet search. For this time, we are about to release Sony Pictures data to the web. The volume of the data is under 100 Terabytes. You can get some of the data at [Links Redacted] We will release all of the data at [XXX and [XXX] in a short time(the minimal time needed for handling tens of TBs of data). The password of the document is "diespe123". Besides, we have much more interesting data than you know. If you Bind special interest, send an email in a method we have explained before. Thanks

December 3st 2014 - “We have released the data of Sony Pictures here”

GOP published the following message:

Hi, We have released the data of Sony Pictures here <http://pastebin.com/zUyA0EiX> And you can Bind data as it adds in PASTEBIN using tags of GOP, SONY, SPE and etc. Today more interesting data will be presented for you. Thanks

December 5st 2014 - “I am the head of GOP”

Two days later, another message from the GOP:

I am the head of GOP who made you worry. Removing Sony Pictures on earth is a very tiny work for our group which is a worldwide organization. And what we have done so far is only a small part of our further plan. It's your false if you think this crisis will be over after some time. All hope will leave you and Sony Pictures will collapse. This situation is only due to Sony Pictures. Sony Pictures is responsible for whatever the result is. Sony Pictures clings to what is good to nobody from the beginning. It's silly to expect in Sony Pictures to take off us. Sony Pictures makes only useless efforts. One beside you can be our member. Many things beyond imagination will happen at many places of the world. Our agents find themselves act in necessary places. Please sign your name to object the false of the company at the email address below if you don't want to suffer damage. If you don't, not only you but your family will be in danger. Nobody can prevent us, but the only way is to follow our demand. If you want to prevent us, make your company behave wisely.

December 6th 2014 - “Gift of GOP for 2nd day”

GOP publish the following message:

You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses. These are all confidential and include data related to sales plan of SPE. <http://torrentproject.se/c8f4990114c6dc96af18f68f0c670a6e141298a6>/magnet:?xt=urn:btih:c8f4990114c6dc96af18f68f0c670a6e141298a6&dn=spe02&tr=<http://retracker.perm.ertelecom.ru/announce>&tr=udp://open.demonii.com:1337/announce&tr=udp://tracker.coppersurfer.tk:6969/announce Password: diespe123

December 7th 2014 - “Gift of GOP for 3rd day Financial data of Sony Pictures”

GOP publishes the following message:

Anyone who loves peace can be our member. Please tell your mind at the email address below if you share our intention. Peace comes when you and I share one intention! 13 jack.nelson-63vrbu1@yopmail.com You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresses. These include many pieces of confidential data. The data to be released next week will excite you more. Password: diespe123

December 8th 2014 - “Gift of GOP for 4th day”

GOP publishes a message targeting Sony executives:

Gift of GOP for 4th day: Their Privacy

```

1 by GOP
2
3 We are the GOP working all over the world.
4 We know nothing about the threatening email received by Sony staffers, but you should wisely judge by yourself why
5
6 Message to SONY
7
8 We have already given our clear demand to the management team of SONY, however, they have refused to accept
9 It seems that you think everything will be well, if you find out the attacker, while no reacting to our de
10 We are sending you our warning again.
11 Do carry out our demand if you want to escape us.
12 And, Stop immediately showing the movie of terrorism which can break the regional peace and cause the War
13 You, SONY & FBI, cannot find us.
14 We are perfect as much.
15 The destiny of SONY is totally up to the wise reaction & measure of SONY.
16
17
18 Their Privacy
19
20 Amy Pascal(Co-Chairman SPE & Chairman MPG), Stephen Mosko(President, SPT)
21
22
23
24 Password: diespe123
25
26 1. Torrent
27 http://rghost.net/59488959
28 http://filesflash.com/x8wxmrfc
29 http://turbobit.net/213ztqlay9d.html
30 http://filenuke.com/f/08dfeL0
31 http://www.uploadable.ch/file/nbPvVgsHgyG/spe\_04.zip
32 http://18upload.com/j50jmcbf16sk
33
34 2. Turbotit
35 http://turbobit.net/up88rjsgg2u7.html
36 http://turbobit.net/cn19fcjz8dyr.html
37 http://turbobit.net/jc5momogicu0u.html
38 http://turbobit.net/561ibejnjd68.html
39
40 3. Filenuke
41 http://filenuke.com/f/6xY23a0
42 http://filenuke.com/f/0nRmk10
43 http://filenuke.com/f/0qgmv53
44 http://filenuke.com/f/3k0Gpgy3
45
46 4. Previous data
47 http://turbobit.net/9n3rvsui7j8.html

```

Pic.16 – GOP announced that Sony refused to accept their “rules of the game”

December 10th 2014 - “Gift of Sony for 5th day: My Life At The Company-Part 1”

GOP publishes the following message:

To SPE employees. SPE employees! Don't believe what the executives of SPE says. They say as if the FBI could resolve everything. But the FBI cannot find us because we know everything about what's going on inside the FBI. We still have huge amount of sensitive information to be released including your personal details and mailboxes. If continued wrongdoings of the executives of SPE drive us to make an unwanted decision, only SPE should be blamed. Now is the time for you to choose what to do. We have already given much time for you.

December 11th 2014 - “Gift of Sony for 5th day: My Life At The Company-Part 2”

GOP publishes the following message:

*by GOP
Important Message to SPE executives
I've sent you a message. Confirm your mailboxes.*

The message is addressed from one person (“I've sent you”). After some time, another message was published:

We are preparing for you a Christmas gift. The gift will be larger quantities of data. And it will be more interesting. The gift will surely give you much more pleasure and put Sony Pictures into the worst state. Please send an email titled by “Merry Christmas” at the addresses below to tell us what you want in our Christmas gift.

December 14th 2014 - “The sooner SPE accept our demands, the better”

GOP released a new message to Sony, promising to bankrupt the company:

The sooner SPE accept our demands, the better, of course. The farther time goes by, the worse state SPE will be put into and we will have Sony go bankrupt in the end. Message to SPE Staffers. We have a plan to release emails and privacy of the Sony Pictures employees. If you don't want your privacy to be released [sic], tell us your name and business title to take off your data.

After the new leaked files were uploaded, former Lizard Squad member “Abdilo” posted:

“Sony could of avoided this if they would pay up the the extortion letter. Take this as a lesson companies, be prepared to loose everything.”¹⁰
(December 17th, “Abdilo”)

December 18th 2014 - “Dear Sony from GOP”

On December 18th, a published post on Pastebin from GOP¹¹, mentioning, “*September 11 may happen again if you don’t comply with the rules*”. The previous day, a Lizard Squad member actively discussed the 9/11 tragic incident in a satirical manner:

Pastebin Post: Dear Sony from GOP

BY A GUEST ON DEC 18TH, 2014 | SYNTAX: NONE | SIZE: 0.38 KB | VIEWS: 8,562 | EXPIRES: NEVER
[DOWNLOAD](#) | [RAW](#) | [EMBED](#) | [REPORT ABUSE](#) | [PRINT](#)

**MANDRILL, TRUSTED FOR EMAIL
INFRASTRUCTURE BY MORE THAN 300,000
CUSTOMERS.**

1. This is GOP.
2.
3. You have suffered through enough threats.
4.
5. We lift the ban.
6.
7. The Interview may release now.
8.
9. But be careful.
10.
11. September 11 may happen again if you don't comply with the rules.
12.
13. Rule #1: no death scene of Kim Jong Un being too happy
Rule #2: do not test us again
Rule #3: if you make anything else, we will be here ready to fight
14.
15.
16.
17.
18. This is Guardians Of Peace.

Twitter Conversation:

@Teridax +||| @AlphaQuintesson · Dec 17
so they're not releasing the interview at all? great

@Teridax +||| @AlphaQuintesson · Dec 17
take it off baby bend over let me see it

View more photos and videos

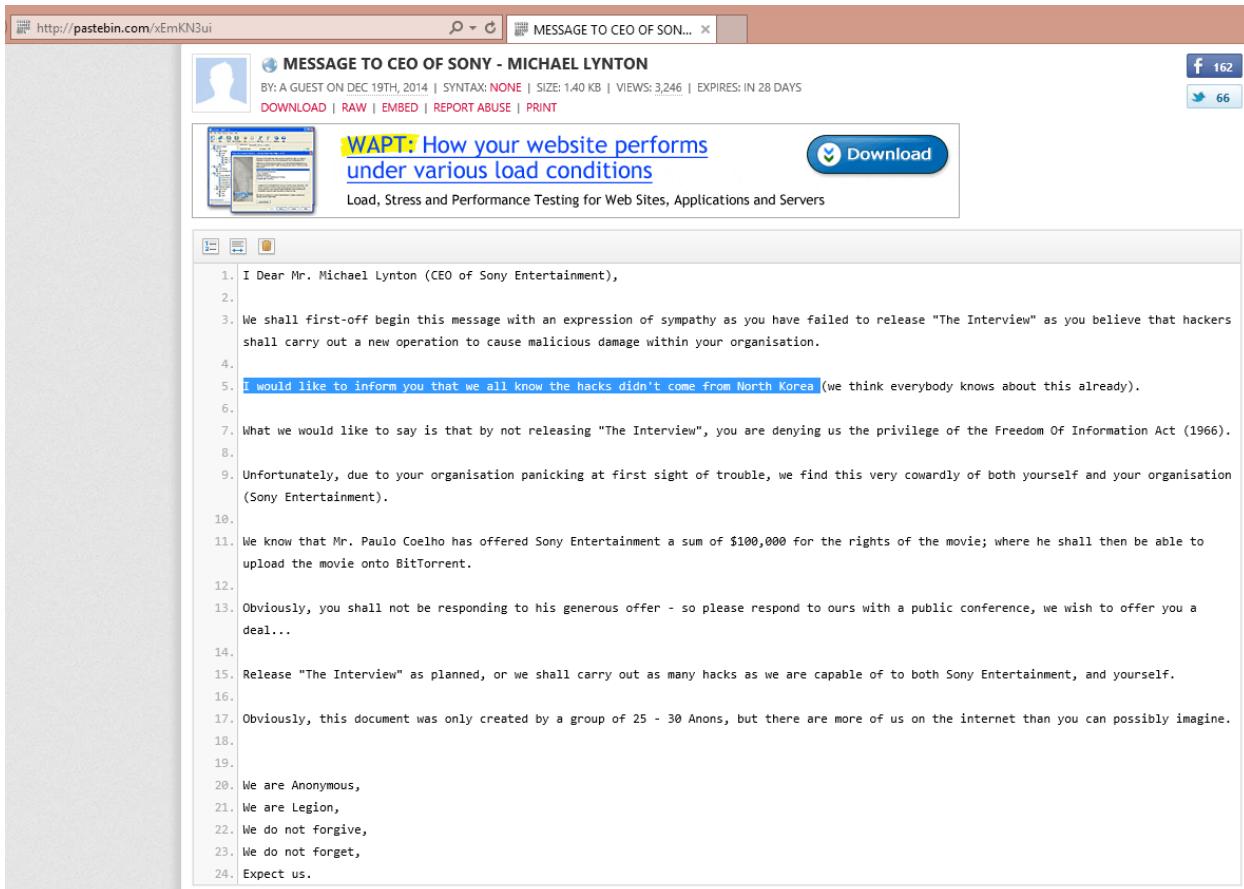
Pic.17 – Lizard Squad member and GOP mentioned the 9/11 incident in their postings

¹⁰ https://twitter.com/abdilo_/status/545456086895960065

¹¹ <http://pastebin.com/m4YB2TJd>

December 19th 2014 - “Message to CEO of Sony - Michael Lynton”

On December 19th there was a published post on Pastebin - <http://pastebin.com/xEmKN3ui>. The bad actors signed the message as “Anonymous” mentioning, “*We all know the hacks didn’t come from North Korea*”:



MESSAGE TO CEO OF SONY - MICHAEL LYNTON

BY A GUEST ON DEC 19TH, 2014 | SYNTAX: NONE | SIZE: 1.40 KB | VIEWS: 3,246 | EXPIRES: IN 28 DAYS

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

WAPT: How your website performs under various load conditions

Load, Stress and Performance Testing for Web Sites, Applications and Servers

Download

1. I Dear Mr. Michael Lynton (CEO of Sony Entertainment),
2.
3. We shall first-off begin this message with an expression of sympathy as you have failed to release "The Interview" as you believe that hackers shall carry out a new operation to cause malicious damage within your organisation.
4.
5. I would like to inform you that we all know the hacks didn't come from North Korea (we think everybody knows about this already).
6.
7. What we would like to say is that by not releasing "The Interview", you are denying us the privilege of the Freedom Of Information Act (1966).
8.
9. Unfortunately, due to your organisation panicking at first sight of trouble, we find this very cowardly of both yourself and your organisation (Sony Entertainment).
10.
11. We know that Mr. Paulo Coelho has offered Sony Entertainment a sum of \$100,000 for the rights of the movie; where he shall then be able to upload the movie onto BitTorrent.
12.
13. Obviously, you shall not be responding to his generous offer - so please respond to ours with a public conference, we wish to offer you a deal...
14.
15. Release "The Interview" as planned, or we shall carry out as many hacks as we are capable of to both Sony Entertainment, and yourself.
16.
17. Obviously, this document was only created by a group of 25 - 30 Anons, but there are more of us on the internet than you can possibly imagine.
18.
19.
20. We are Anonymous,
21. We are Legion,
22. We do not forgive,
23. We do not forget,
24. Expect us.

Pic.18 – One of the first messages to Sony from hackers with Anonymous signature

After this post, new independent Hacktivists appeared, with some participating and promoting “Anonymous” and starting #OpSony campaign.

CWN follows
Anon Pyro @AnonPyr0 · Dec 27
 Many thanks to @AnonSecurity_ and @Global_hackers for working on #OpSony with me
 11 9 ...

Charles Ibrahim and 6 others follow
#GHC_sec @Global_hackers · Dec 27
 Open fire:
 Sony pictures need to be downed
 IP: 72.52.12.83 (apache server)
 Port(s): 80 / 443 open
 #ANONFAMILY: fire your lasers for #OpSony
 5 3 ...

CWN @Cyber_War_News · Dec 27
 uh oh cwn.link/1vBaJje is being hit again via #opsony ... amazingly not one bit of lag
 2 1 ...

Favourited 32 times
AnonSec @AnonSecurity_ · Dec 27
 For the final time I will say it again. We are NOT firing at PSN. We are firing at Sony Pictures. #OpSony
 30 32 ...

AnonSec @AnonSecurity_ · Dec 27
 FIRE
 TARGET: sonypictures.com
 IP: 72.52.12.83 (apache server)
 Port(s): 80 / 443 open
 #Anonymous #OpSony

YouTube
 ANONYMOUS #OpSony LAUNCH VIDEO



#OpSony
 0:27

ANONYMOUS #OpSony
 WE ARE ANONYMOUS. WE DON'T FORGIVE. WE DON'T FORGET. SONY, EXPECT US. Reason for attacks: Sony Pictures lied to the public about being 'hacked' by North Kore...

Pic.19 – #OpSony will be targeted on DDoS against Sony Pictures

On the same day, former member of “Lizard Squad” mentions “GOP” and current investigation in satirical form:

abdilo @abdilo_

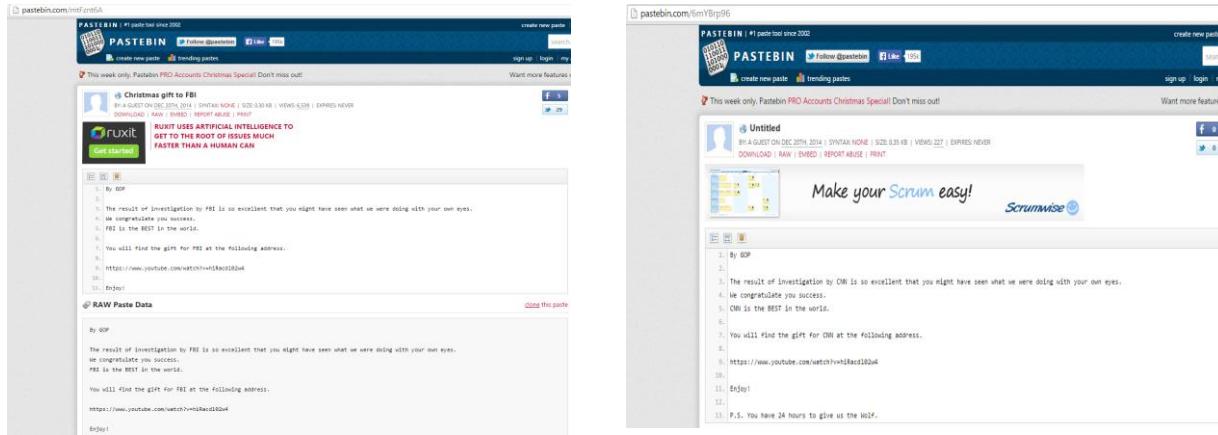
Ok so apparently the fbi considers doxing and ddosing worse then murder, espionage, GoP, fraud, assault... oh wait

2 12:19 am - 19 Dec 2014

Pic.20 – Former Lizard Squad member “Abdilo” mentioned GOP

December 20th 2014 - “Christmas gift to FBI”

After the new FBI update on the Sony hack¹², two published posts by GOP denied any link with North Korea:



Pic.21 – GOP will deny the link with North Korea in “Christmas gift” post

December 22th 2014 - “Working together with GOP on a Christmas project”

Lizard Squad published a post that they work with GOP¹³ on a Christmas project:

¹² <http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>

¹³ <https://twitter.com/LizardUnit/status/546752455661584385>



Lizard Squad
@LizardUnit

Next generation Grinch. Cyber terrorists labelled as a matter of national security. Once upon a time @LizardPatrol and @LizardSquad.

XMPP/Email: lizards@riseup.net
chat.lizardpatrol.com

[Tweet to Lizard Squad](#)

TWEETS 19 FOLLOWING 9 FOLLOWERS 9,686 FAVOURITES 12

Tweets Tweets & replies

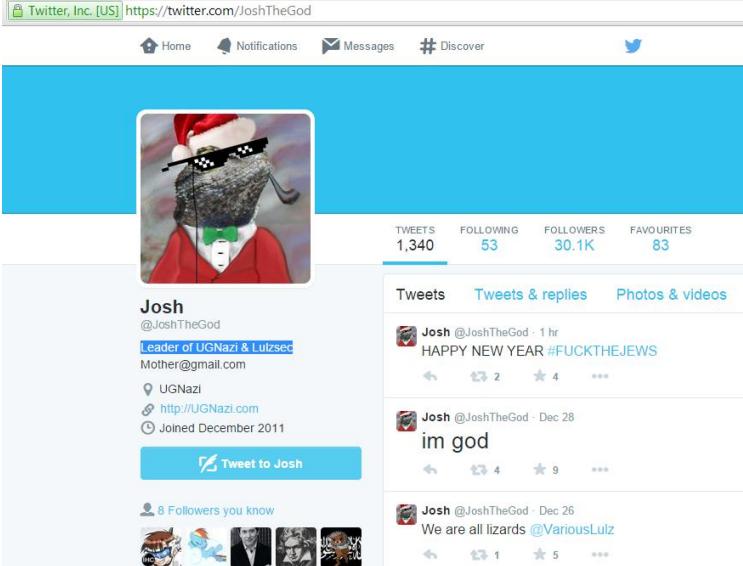
Lizard Squad @LizardUnit - 2 hrs
Jabber/Email: lizards@riseup.net
5 12 ...

Lizard Squad @LizardUnit - 3 hrs
Working together with #GoP on a Christmas project.
16 32 ...

Lizard Squad @LizardUnit - Dec 19

Pic.22 – Lizard Squad announced work with GOP

An interesting fact is that the avatar of Lizard Squad is used by other hacking groups and their leaders, such as “JoshTheGod”. This bad actor named himself as “Leader of UGNazi & LulzSec”, groups that compromised Sony in 2011.



Josh
@JoshTheGod

Leader of UGNazi & LulzSec
Mother@gmail.com

UGNazi
<http://UGNazi.com>
Joined December 2011

[Tweet to Josh](#)

TWEETS 1,340 FOLLOWING 53 FOLLOWERS 30.1K FAVOURITES 83

Tweets Tweets & replies Photos & videos

Josh @JoshTheGod - 1 hr
HAPPY NEW YEAR #FUCKTHEJEWS
2 4 ...

Josh @JoshTheGod - Dec 28
im god
4 9 ...

Josh @JoshTheGod - Dec 26
We are all lizards @VariousLulz
1 5 ...

Pic.23 – Leader of UGNazi & LulzSec with the same avatar as Lizard Squad

Later, the Lizard Squad member, “Abdilo” explained that he left the group in October 2014, but retained relations with team members. Lizard Squad mentions GOP in some of their posts:

<https://twitter.com/LizardMafia/status/547570060160954369>
"greets from DPRK ;)==="

<https://twitter.com/LizardMafia/status/547579229156954112>
 "We should do it too every channel. Greets to GoP & DPRK"



We should do it too every channel. Greets to GoP & DPRK

[Like](#) · [Comment](#) · [Share](#)

Pic.24 – Lizard Squad will greet GOP and DPRK (North Korea)

During active discussions of a possible film leak “The Interview”, The Pirate Bay was defaced with picture of North Korea leader. “Abdilo” mentioned this incident with an ambiguous phrase: “GOP you trolls”.

THN [The Hacker News](#) @TheHackersNews · 3h
 'The Pirate Bay' HACKED? N.Korea' Kim Jong Un Cartoon Appears on Homepage. thn.li/7ky5 | #thepiratebay pic.twitter.com/Fx28FKohHB

70 17

abdilo @abdilo_ · 5:38 am - 27 Dec 2014

.@TheHackersNews @hue
 AHHAHAHAHAHAHAAHAHAHHA GOP you
 trolls

1

Pic.25 – “GOP you trolls” comment by Abdilo

December 29th 2014 - “Well, we do know some people from the GOP”

In an interview with the Washington Post¹⁴, Lizard Squad explained, that they have links with “GOP” and provided the group with credentials for Sony hack:

Q: Some reports suggest you've got links to Guardians of Peace, and possibly to the Islamic State. Can you talk about that for a minute?

[Another long pause, about five minutes.]

A: Well, we do know some people from the GOP. We do not have any links to the IS.

Q: But you didn't work with Guardians of Peace to breach Sony's network and gain access to the e-mails, etc.? In other words, you know some people but weren't involved in the Sony hack surrounding 'The Interview'?

[A seven-minute pause.]

A: Well, we didn't play a large part in that.

Q: What part did you play?

A: We handed over some Sony employee logins to them. For the initial hack.

December 30th 2014 - “Looking at this south korean powerplant”

“Abdilo” has mentioned South Korean nuclear energy company KHPN, which was referenced in a Reuters article about a hacking attempt and leak of documents.

Computer systems at South Korea's nuclear plant operator have been hacked, the company said on Monday, sharply raising concerns about safeguards around nuclear facilities in a country that remains technically at war with North Korea (Reuters, December 22nd 2014)

¹⁴ <http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/29/a-qa-with-the-hackers-who-say-they-helped-break-in-to-sonys-network/>



abdilo @abdilo Dec 31
So Argentina gives me access to their airforce and south korea lets me kill all of their citizens.... thanks asp

abdilo @abdilo Dec 30
cms.khnp.co.kr/readme.html :]

abdilo @abdilo Dec 30
/NAS_Vol/www/khnp/wp-content/themes/khnp/index.php
roflmao

abdilo @abdilo Dec 30
and they have wordpress.....

abdilo @abdilo Dec 30
Looking at this south korean powerplant that was rekt... dear god the jpg

Pic.26 – Former Lizard Squad member “Abdilo” and vulnerabilities in KHNP

abdilo
@abdilo_

Nuclear systems are fun to mess with, what happens when i turn the fans off.....

FAVOURITE
1

3:00 am - 5 Dec 2014

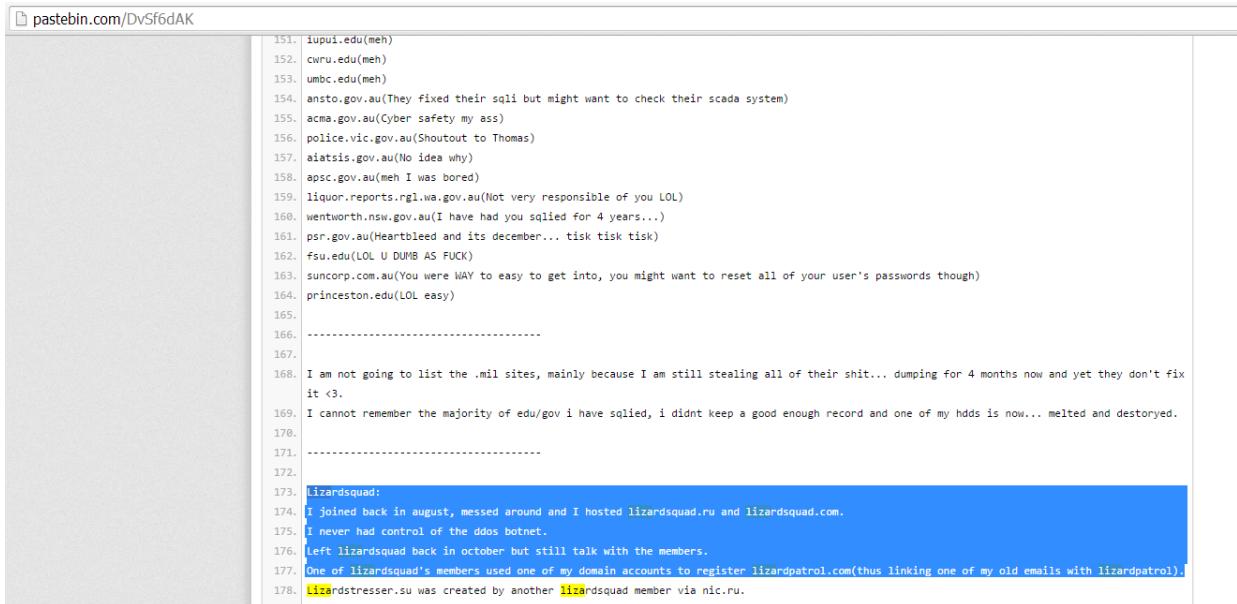
Pic.27 – The bad actor started his harmful activities in early December

December 31th 2014 - “Suicide Hacking in Australia”

The bad actor “Abdilo” published a very specific post on Pastebin about his past cyber attacks (URL: <http://pastebin.com/DvSf6dAK>).

He enumerated some of his hacked targets in the past, and explained that he left Lizard Squad in October, but retained relations with its members.

Now I am going to attack south korea... one uni now has no records, no mssql db, none of its asp/aspx and all external hdds have been formatted. (31st December 2014, “Abdilo”)



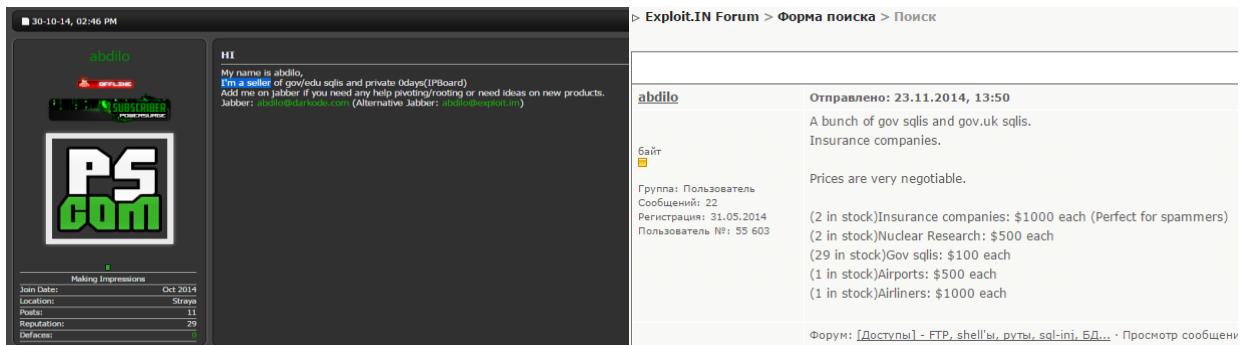
```

151. iupui.edu(meh)
152. cwrw.edu(meh)
153. umbc.edu(meh)
154. ansto.gov.au(They fixed their sqls but might want to check their scada system)
155. acma.gov.au(Cyber safety my ass)
156. police.vic.gov.au(Shoutout to Thomas)
157. aiatssis.gov.au(No idea why)
158. apsc.gov.au(meh I was bored)
159. liquor.reports.rgl.wa.gov.au(Not very responsible of you LOL)
160. wentworth.nsw.gov.au(I have had you sqlied for 4 years...)
161. psr.gov.au(Heartbleed and its december... tisk tisk tisk)
162. fsu.edu(LOL U DUMB AS FUCK)
163. suncorp.com.au(You were WAY to easy to get into, you might want to reset all of your user's passwords though)
164. princeton.edu(LOL easy)
165.
166.
167.
168. I am not going to list the .mil sites, mainly because I am still stealing all of their shit... dumping for 4 months now and yet they don't fix it <3.
169. I cannot remember the majority of edu/gov i have sqlied, i didnt keep a good enough record and one of my hdds is now... melted and destroyed.
170.
171.
172.
173. lizardsquad:
174. I joined back in august, messed around and I hosted lizardsquad.ru and lizardsquad.com.
175. I never had control of the ddos botnet.
176. left lizardsquad back in october but still talk with the members.
177. One of lizardsquad's members used one of my domain accounts to register lizardpatrol.com(thus linking one of my old emails with lizardpatrol).
178. Lizardstresser.su was created by another lizardsquad member via nic.ru.

```

Pic.28 – Published list of hacked government resources by “Abdilo”

In October 2014, “Abdilo” started advertising his own services in the underground, related to the selling of vulnerabilities on government WEB-sites and private exploits.



30-10-14, 02:46 PM

abdilo

HI
My name is abdilo,
I'm a seller of .gov/.edu sqls and private 0days(IPBoard)
Add me on jabber if you need any help pivoting/rooting/ or need ideas on new products.
Jabber: abdiloweb@jabber.com (Alternative Jabber: abdiloweb@pricenet.com)

Join Date: Oct 2014
Location: Straya
Status: 1
Reputation: 29
Defaces: 0

Exploit.IN Forum > Форма поиска > Поиск

abdilo Отправлено: 23.11.2014, 13:50
A bunch of gov sqls and gov.uk sqls.
Insurance companies.
Prices are very negotiable.
(2 in stock)Insurance companies: \$1000 each (Perfect for spammers)
(2 in stock)Nuclear Research: \$500 each
(29 in stock)Gov sqls: \$100 each
(1 in stock)Airports: \$500 each
(1 in stock)Airliners: \$1000 each

Форум: [\[Доступны\] - FTP, shell'ы, руты, sql-inj, БД...](#) · Просмотр сообщения

Pic.29 – “Abdilo” began advertising his own hacking services of .gov/.edu resources in the underground

<pre> 182. ----- 183. 184. Here are some of the sites I messed with: 185. every *.k12 site is vuln to sql injection. 186. cdc.gov(what kind of db do you even use! still have a sql in your but cannot figure it out) 187. longbeach.gov(I HAS INFORMATION ABOUT COSMO BEING A PED... look! just fucking with ya) 188. ny.gov(Shoutout to teriidae shane there was no proof of 9/11 attacks XD) 189. metrolstate.edu(I broke into you cause I like 22 jump street, thanks for the 22k ssns) 190. MSU.edu(no reason) 191. cam.ac.uk(Fuck steven haulings) 192. liv.ac.uk(Too slow my ass) 193. stardard.education guy found a sql in you then I found a better one... fuck you 194. yale.edu(what) 195. ncsu.edu(there's for the bc soils digitalagenter.com loved it LOL) 196. arizona.edu(I called you 4 times while onnoxious called you up on the phone to troll you and tell you, then dumping your database 4 times then asking for booty pix else we release it) 197. texas.gov(Shoutout to CosmoTheGod) 198. mo.gov((cause why not)) 199. virginia.gov(Hi Ryan F) 200. louisiana.gov(You have up_cmshell thank you) 201. dc.gov(Someone I know got scammed by some cunt in dc... so why not attack the .gov >>)) 202. catholic.edu.au(Fuck Catholics) lol I have no reason I just did it for the hell of it) 203. goodnews.vic.edu.au(Badnews I has all ur records) 204. goodshepherd.edu.au(Badnews are all christian schools vuln to sql besides liberty.edu) 205. mercy.vic.edu.au(MERCY FOR YOU) 206. spauliba.sa.edu.au(... I have nothing funny to say lol) 207. stjosephbrackenridge.cld.edu.au(Seriously another christian school) 208. gatech.edu(Nice alexa rank) 209. uky.edu(you are yucky) 210. vmi.edu(fuck you have a shit alexa rank) 211. miami.edu(I was watching dealer and wanted to get into your police station... this was close enough for me) 212. berkeley.edu(you fixed it don't worry, tuas funny having a sql in a 1.5k alexa rank site) 213. seattle.gov(Dam I lulznow level now! LOL, Fuck IBM DB) 214. case.edu(Fuck the law) 215. ----- </pre>	<p>abdilo Байт</p> <p>Группа: Пользователь Сообщений: 22 Регистрация: 31.05.2014 Пользователь №: 55 603</p>	<p>Отправлено: 26.10.2014, 09:57</p> <p>Gov sites(\$100 each): mo.gov virginia.gov louisiana.gov</p> <p>Edu sites(\$50 each): gatech.edu uky.edu vmi.edu miami.edu berkeley.edu</p> <p>Форум: [Доступы] - FTP, shell'ы, руты,</p>
<p>texas.gov sqld by abdilo BY A GUEST ON DEC 18TH, 2014 SYNTAX: NONE SIZE: 541 KB VIEWS: 192 EXPIRES: NEVER DOWNLOAD RAW EMBED REPORT ABUSE PRINT</p> <p>HipChat HipChat Means Business. Instant messaging, video chat, file sharing & more. Get it free</p> <p>texas.gov sqld by abdilo BY A GUEST ON DEC 18TH, 2014 SYNTAX: NONE SIZE: 3.90 KB VIEWS: 529 EXPIRES: NEVER DOWNLOAD RAW EMBED REPORT ABUSE PRINT</p> <p>codeup THE ELITE PROFESSIONAL SCHOOL FOR COMPUTER PROGRAMMING. 4 AND 12 MONTH PROGRAMS.</p>	<p>dc.gov sqld by abdilo BY A GUEST ON DEC 18TH, 2014 SYNTAX: NONE SIZE: 3.90 KB VIEWS: 529 EXPIRES: NEVER DOWNLOAD RAW EMBED REPORT ABUSE PRINT</p> <p>codeup THE ELITE PROFESSIONAL SCHOOL FOR COMPUTER PROGRAMMING. 4 AND 12 MONTH PROGRAMS.</p>	<p>texas.gov sqld by abdilo BY A GUEST ON DEC 18TH, 2014 SYNTAX: NONE SIZE: 541 KB VIEWS: 192 EXPIRES: NEVER DOWNLOAD RAW EMBED REPORT ABUSE PRINT</p> <p>dc.gov sqld by abdilo BY A GUEST ON DEC 18TH, 2014 SYNTAX: NONE SIZE: 3.90 KB VIEWS: 529 EXPIRES: NEVER DOWNLOAD RAW EMBED REPORT ABUSE PRINT</p>

Pic.30 – Published samples of compromised government resources

Besides government segment, he has also published for sale information about vulnerabilities in regard of leading insurance companies of Australia – SunCorp and GIO Insurance Australia.

abdilo  Байт  Группа: Пользователь Сообщений: 22 Регистрация: 31.05.2014 Пользователь №: 55 603	Отправлено: 17.11.2014, 11:26 Selling sql in suncorp.com.au Add on jabber for more info(price is negotiable) Company Info: Suncorp Group includes leading general insurance, banking, life insurance and superannuation brands in Australia and New Zealand. The Group has 15,000 employees and relationships with nine million customers. We are a Top 20 ASX-listed company with \$96 billion in assets Jabber: abdilo@darkode.com Price: \$5,000 Форум: [Последний] - FTP, shell'ы, руты, sql-inj, БД... · Просмотр сообщения: #513439 · Ответов: 1 · Просмотров: 76
abdilo  Байт  Группа: Пользователь Сообщений: 22 Регистрация: 31.05.2014 Пользователь №: 55 603	Отправлено: 17.11.2014, 11:22 Selling sql in suncorp.com.au Add on jabber for more info(price is negotiable) Company Info: Suncorp Group includes leading general insurance, banking, life insurance and superannuation brands in Australia and New Zealand. The Group has 15,000 employees and relationships with nine million customers. We are a Top 20 ASX-listed company with \$96 billion in assets Jabber: abdilo@darkode.com

According to gathered information, he has compromised more than 60 government and educational WEB-resources, the majority of which were published in his posts¹⁵.

I am not going to list the .mil sites, mainly because I am still stealing all of their shit... dumping for 4 months now and yet they don't fix it <3. I cannot remember the majority of edu/gov i have sqlied, i didnt keep a good enough record and one of my hdds is now... melted and destoryed.

(December 31th, "Abdilo")

During long term monitoring of the Lizard Squad IRC channel, several messages were identified referencing the hacking of military and government resources. This verifies that the objects of interests of the bad actors are not limited to gaming services only.

Pic.31 – Analyzed communications from Lizard Squad channel and compromised military WEB-resources

¹⁵ <http://pastebin.com/DvSf6dAK>

In his Twitter account, he mentions, that his future hacking activities will be targeted on South Korea - https://twitter.com/abdilo_/status/550466414897684483

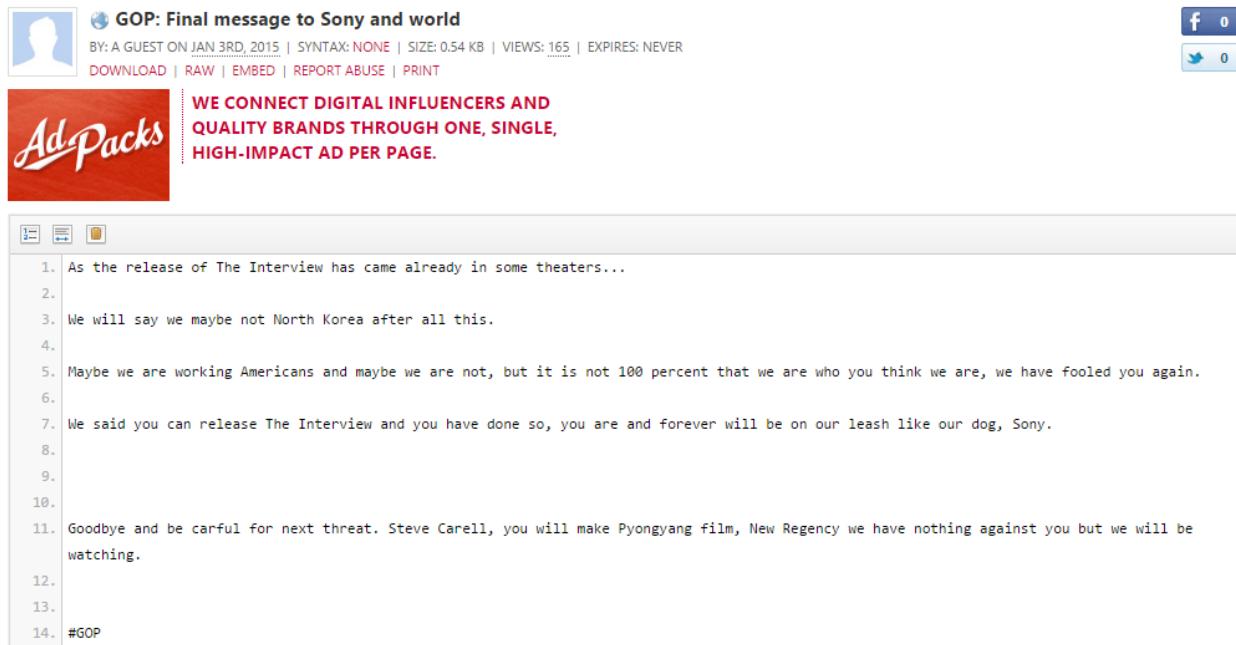
The image shows three Twitter posts. The first post is from user @abdilo_ (@abdilo_) at 11:26 PM - 27 Dec 2014. The text reads: "Hmm, usa, aus, uk, argentina, iran, israel, etc... now lets mess with south korea". The second post is from the same user at 5:39 PM - 31 Dec 2014. The text reads: "So all of 2014 was dedicated to sqling usa/aus's gov/mil/nuclear/edu... 2015 will be dedicated to sqling all of south korea". The third item is a reply from user @RHElijah (@RHElijah) at 5:39 PM - 31 Dec 2014, with the text: "[RICH HOMIE] Elijah @RHElijah - Dec 31 @abdilo_ have a jabber or something lol". Each post includes standard Twitter interaction icons (retweet, favorite, etc.) and a 'Follow' button.

Pic.32 – “Abdilo” will target his illegal activities against South Korea for reasons unknown

Provided facts may point at specifics surrounding the personal motivation of “Abdilo” and undisclosed customers of his services, who could use the results of his work for harmful activities.

January 3^d 2015 - “GOP: Final message to Sony and world”

There was published anonymous post with the same style of text, signed by “GOP”¹⁶.



GOP: Final message to Sony and world

BY: A GUEST ON JAN 3RD, 2015 | SYNTAX: NONE | SIZE: 0.54 KB | VIEWS: 165 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

**WE CONNECT DIGITAL INFLUENCERS AND
QUALITY BRANDS THROUGH ONE, SINGLE,
HIGH-IMPACT AD PER PAGE.**

1. As the release of The Interview has came already in some theaters...

2.

3. We will say we maybe not North Korea after all this.

4.

5. Maybe we are working Americans and maybe we are not, but it is not 100 percent that we are who you think we are, we have fooled you again.

6.

7. We said you can release The Interview and you have done so, you are and forever will be on our leash like our dog, Sony.

8.

9.

10.

11. Goodbye and be carful for next threat. Steve Carell, you will make Pyongyang film, New Regency we have nothing against you but we will be watching.

12.

13.

14. #GOP

Pic.33 – One of the latest messages, signed by GOP, after Sony hack

¹⁶ <http://pastebin.com/DZcSzy6N>

Appendix A. - Lizard Squad / GOP Characteristics

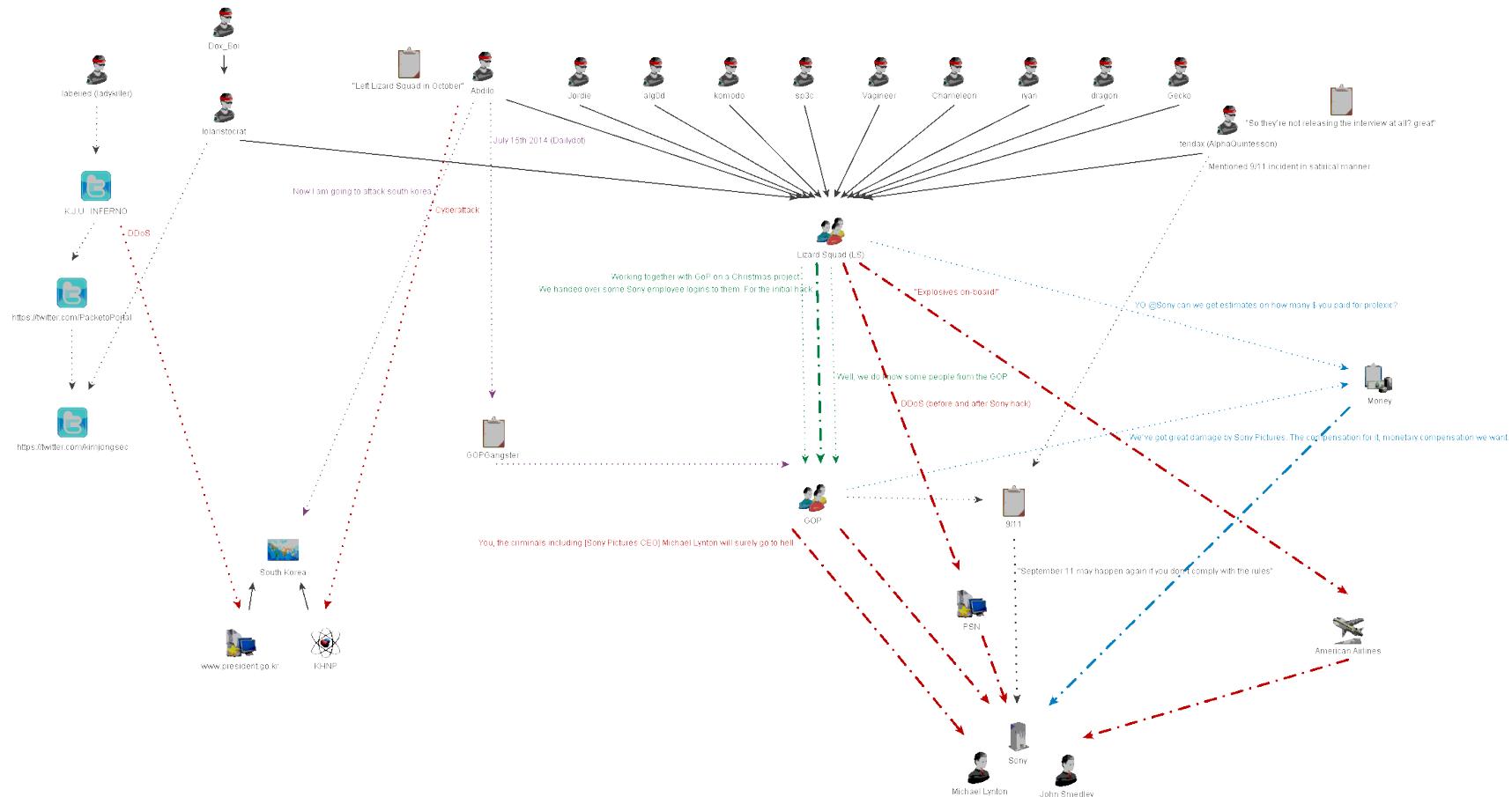
#	Lizard Squad	GOP
1	Lizard Squad has a leader, and group of hackers, performing cyber attacks.	GOP has a leader, calling himself “boss” or “head”, coordinating other members.
2	Lizard Squad members are from the UK, Australia, Sweden and Finland, having fluent English.	GOP uses pretty good English in each of their messages to Sony, it doesn’t have any incorrect translation and written in quite fluent form.
3	Lizard Squad member “Abdilo” has registered several domains in .RU, including official WEB-site of the group.	GOP used .RU server, besides others, where they have uploaded leaked files. Potentially, this server was compromised in the past.
	Lizard Squad member “Abdilo” left Lizard Squad in October 2014.	GOP released information about Sony in late November 2014.
4	Lizard Squad has threatened the victims with “ <i>wonderful present to Christmas</i> ”. They also announced “ <i>Working together with #GoP on a Christmas project</i> ”.	GOP has threatened Sony with “ <i>Christmas gift</i> ” too, which shows a correlation in timeline development and approach in dialogue with victims.
5	Lizard Squad member “Abdilo” has a GitHub account.	GOP has published several messages in GitHub, containing specifics.
6	Lizard Squad messages directly addressed to Sony several times, mentioning some commercial topics: <i>Sony, yet another large company, but they aren't spending the waves of cash they obtain on their customers' PSN server. End the greed.</i> <i>YO @Sony can we get estimates on how many \$ you paid for prolexic?</i>	GOP messages addressed directly to Sony every time, including money compensation in order to prevent potential damage: <i>We've got great damage by Sony Pictures. The compensation for it, monetary compensation we want.</i>
7	December 17 th , Lizard Squad member “teridax” actively discussed 9/11 tragic incident in a satirical manner.	December 18 th , GOP has published a post with phrase “ <i>September 11 may happen again if you don't comply with the rules</i> ”.
8	Lizard Squad has words about North	GOP has mentioned the North Korean

	Korea at the end of their official song: “ <i>North Korea...is the best Korea</i> ” ¹⁷	President in several of their posts. “ <i>No death scene of Kim Jong Un being too happy</i> ”.
9	Sony was hacked by LulzSec in 2011. Lizard Squad affiliates have some members from other groups, such as “UGNazi” and “ex-LulzSec”, using the same symbolic and style of posts. After the arrest of LulzSec members, the group was restructured.	So called “GOP” who compromised Sony in 2014, previously had no hacking activities or presence in the WEB.
10	Immediately after the Sony hack, Lizard Squad repeated DDoS attack on Sony PSN.	There is a correlation in harmful activities from Lizard Squad and GOP by time.
11	In an interview with the Washington Post, Lizard Squad explained, that they have links with “GOP” and provided them with credentials for the Sony hack. <i>Well, we do know some people from the gop. We handed over some Sony employee logins to them. For the initial hack.</i>	There is a correlation in harmful activities from Lizard Squad and GOP by means of attack, and by the fact, that one of Lizard Squad members “Abdilo” left the group in October 2014, before the Sony hack, which may show him as one of the potential bad actors, responsible for the new group GOP and past attacks.
12	In one of the articles, relating to the first DDoS attacks on big e-gaming services, there was a mentioned actor “GOPGangster”. Lizard Squad member “Abdilo”, using one of his old nicknames, commented the article.	There is a correlation between GOP as a group name, and links between Lizard Squad former member “Abdilo” and “GOPGangster”.

. **Table 2** – Lizard Squad / GOP Characteristics Analysis

¹⁷ https://www.youtube.com/watch?v=fS3cVh_vtsc

Appendix B. - Social Graph



Conclusion

Our analysis shows that young gamers were dissatisfied for a variety of reasons with the technology companies that provided them participating networks.

Attacking companies for fun, for a challenge, for a disliked policy, is really the ultimate online game. These identified bad actors seemed to have penetrated the networks over a substantial time period, giving them access to all types of intellectual property, corporate assets, and employee data. As discovered, these access points were offered up for sale or trade in the underground.

These groups are not solely restricted to the gaming sector but are clearly demonstrating their pursuit in other objects of interest.

The recent high profile targeted cyber attacks may have involved "for hire" hacker groups or independent Hacktivists.

Disclaimer

The research, findings, and analysis in this report are based on a combination of open and operative sources. To protect some victims and open cases, the non-disclosure of operative sources may leave some gaps in the linkage of some parts of the analysis. This report is solely the opinion of IntelCrawler LLC.

Trademarks

IntelCrawler, the IntelCrawler logo, and IntelCrawler's products and services are trademarks or registered trademarks of IntelCrawler LLC. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or the names of their products. IntelCrawler disclaims proprietary interest in the marks and names of others.

© Copyright 2015 IntelCrawler LLC. All rights reserved.